Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform*

Xiao-ling HUANG, You-xia DONG, Kai-xin JIAO, Guo-dong YE†‡

Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China

†E-mail: guodongye@hotmail.com

Received May 20, 2020; Revision accepted Sept. 21, 2020; Crosschecked Oct. 29, 2020

Abstract: We propose a new asymmetric pixel confusion algorithm for images based on the Rivest-Shamir-Adleman (RSA) public-key cryptosystem and Arnold map. First, the RSA asymmetric algorithm is used to generate two groups of Arnold transform parameters to address the problem of symmetrical distribution of Arnold map parameters. Second, the image is divided into blocks, and the first group of parameters is used to perform Arnold confusion on each sub-block. Then, the second group of parameters is used to perform Arnold confusion on the entire image. The image correlation is thereby fully weakened, and the image confusion degree and effect are further enhanced. The experimental results show that the proposed image pixel confusion algorithm has better confusion effect than the classical Arnold map based confusion and the row-column exchange based confusion. Specifically, the values of gray difference are close to one. In addition, the security of the new confusion operation is dependent on RSA, and it can act as one part of a confusion-substitution structure in a cipher.

Key words: Rivest-Shamir-Adleman (RSA); Arnold map; Pixel confusion; Asymmetric algorithm; Image confusion

https://doi.org/10.1631/FITEE.2000241 **CLC number:** TP37

1 Introduction

Digital images are increasingly integrated into people's lives and play an increasingly important role in communication. Because digital images can be transmitted through communication tools, e.g., computers and mobile devices, it is possible for them to be stolen in the communication process. Unfortunately, traditional encryption algorithms, e.g., the Advanced Encryption Standard (AES) (Mossa, 2017; Arab et al., 2019) and Data-Encryption Standard (DES) (Mitchell, 2016), have poor image encryption efficiency because of the high redundancy and strong correlation of digital images (Gan et al., 2019; Li et al., 2019).

Cryptography can be divided into symmetric and asymmetric types. Because of their advantages of high security and easy digital signature and verification implementations, asymmetric cryptography algorithms have been extensively researched (Verma et al., 2019). Wu et al. (2019) suggested a new image compression and encryption scheme, in which a discrete wavelet transform (DWT) is employed together with nonlinear operations. It is more conductive for data transmission using DWT. In Wu's scheme, four component images for a greyscale image are obtained after applying DWT. Then, the scheme can obtain a single-amplitude ciphertext when nonlinear phase truncation is processed followed by a

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 61972103 and 61702116), the Natural Science Foundation of Guangdong Province, China (No. 2019A1515011361), the Project of Enhancing School with Innovation of Guangdong Ocean University (No. Q18306), and the Guangdong Postgraduate Education Innovation Project (No. 2020JGXM059)

ORCID: Xiao-ling HUANG, https://orcid.org/0000-0001-6129-1188; Guo-dong YE, https://orcid.org/0000-0003-4222-1824

© Zhejiang University and Springer-Verlag GmbH Germany, part of Springer Nature 2020

cylindrical diffraction. Yao et al. (2017) proposed an asymmetric method to encrypt a colour image through the deduced gyrator transform (GT). Using a GT algorithm, by multiplying a phase distribution and performing Fourier transform (FT), the spectrum modulus of the input image is treated as the encrypted image. To avoid the attack in an iterative phase-retrieval way, a random phase mask is used to modulate three components (i.e., red, green, and blue) in the input image with a function of convolution. Then, for convenient display, transmission, and storage, all values in the image are quantized to a real value. Using a correct decryption key, the original colour plain image can be obtained after the three original color components red, green, and blue are recovered. Xiao et al. (2017) designed a high-payload joint reversible data-hiding scheme. To be different from traditional methods, the data hider embeds the data through flipping the most significant bits (MSBs) after the owner estimates the content and generating a location map. To overcome the problems of user inconvenience, low efficiency, and low security level, Khashan et al. (2015) proposed a concept of "transparent encryption."

The RSA algorithm (Boldyreva et al., 2010) is a representative of asymmetric cryptography, and has been widely used in public-encryption systems. It has the advantages of ease of use, fast data transmission, and high management convenience, and can resist the vast majority of password attacks known thus far. To improve the security of an image-encryption system, Gong et al. (2019b) proposed a new compression and encryption scheme for optical images using compressive sensing and the RSA public-key cryptographic algorithm. To sample the original image, an optical compressive imaging system was employed, simulated by Walsh-Hadamard transform and a measurement matrix. To enhance the security, a pseudo-random sequence was used to scramble the related positions for image pixels in the resulting image. Then, all values were further modulated by a random DNA sequence. Because of the relationship between the key and the original image under the RSA algorithm, the encryption algorithm can achieve good performance.

El-Khamy et al. (2017) used RSA encryption technology and the DWT domain for image hiding encryption, and wrote it into an audio steganography algorithm. This method encrypts the plaintext image with RSA, and then embeds the cipher bits into detailed components of the audio signals according to a predetermined threshold. However, because of the transformation domain, the image cannot be fully restored. Two basic principles of the digital-image encryption design are scrambling and diffusion. To address the shortcomings of the Fridrich structure, for example, the gray distribution maintained before the diffusion operation, an efficient pixel-level chaotic image-encryption algorithm has been proposed by Ye et al. (2018). The permutation-rewrite-diffusion (PRD) structure was used to simply rewrite the permutation image before the diffusion operation. The key-stream design depends on displacement and diffusion operations being applied to the original image, to avoid known-plaintext and selective-plaintext attacks.

To reduce extra transmission in the encryption algorithm, Ye and Huang (2018) suggested to use random confusion methods for pure images with the help of pixel frequencies, followed by two diffusion operations to change the pixel distribution. Hua et al. (2019) used the Joseph principle to shuffle the image pixels to different positions and achieved good confusion effect. The filtering technique uses a randomly generated filter to propagate small changes in the original image to all the pixels of the encrypted image to obtain the diffusion characteristics. Chen JX et al. (2018) used adaptive permutation-diffusion and random DNA encoding to achieve secure and efficient image encryption. A random DNA encoding was used to scramble the plaintext's bit distribution, and then an adaptive permutation-diffusion process was introduced for further encryption. The quantisation processes of the permutation and diffusion procedures were disturbed by the intrinsic features of the plaintext, and the introduced disturbances can be automatically retrieved at the end of the decryption. Yu et al. (2020) proposed a chaotic image-encryption algorithm based on the phase-truncation short-time fractional Fourier transform (PTSTFrFT). The sub-images obtained by decomposing the original images were encoded with encryption units. By combining the PTSTFrFT with a wave-based permutation, an encryption unit was constructed to encode the sub-images, and the mixed-phase information and amplitude information were recombined, to ensure the integrity of image information and the nonlinearity of phase truncation. Then, the pixel values

and positions were modified by permutation and diffusion operations to generate an interim image.

Because the Arnold transform is intuitive and simple, it is commonly used in image-confusion algorithms (Chen LF et al., 2013; Liu LF et al., 2018; Mansouri and Wang, 2020; Sneha et al., 2020). One algorithm based on a generalized Arnold transform and double-random-phase encoding (Zhou et al., 2015) combines the Arnold transform and a double-random-phase encoding technique. It uses the double-random phase to perform diffusion, and the Arnold transform to mix the pixels. Arnold transform increases the number of keys and improves the security. Zhu ZL et al. (2011) replaced high four-bit planes with low bit planes to reduce the execution time. They used the Arnold map for permutation and diffusion. This approach uses bit permutation and diffusion to provide good security against chosen/known plaintext attacks. To reduce the blocking effect in the compression process, another algorithm (Gong et al., 2019a) performs Arnold scrambling on the image before compressing and encrypting it. One digital image-encryption method uses a structural random matrix and the Arnold transform (Rawat et al., 2016). The Arnold transform was used to convert the reduced digital image into a more complex form, which was then encrypted by a double-random-phase encoding process and embedded into a host image. Liu ZJ et al. (2012) designed a double-image-encryption algorithm based on the Arnold transform and discrete fractional angular transform. Two original images were regarded as the amplitude and phase of a complex function. The Arnold transform was introduced to scramble the pixels at a local area of the complex function. Subsequently, the changed complex function was converted by a discrete fractional angular transform.

Unlike traditional applications of the symmetric Arnold map, this study combines the RSA algorithm and Arnold map to produce an asymmetric image-pixel confusion algorithm. This ensures the security of the algorithm using the large-integer factorization problem. The Arnold map cycle is effectively prolonged by local (sub-block) and global (whole block) confusion.

The contributions of this paper are as follows:

1. combination of asymmetric RSA with the symmetric confusion technology of an Arnold map;

2. application of double confusion operations to both the sub-blocks and the entire image to extend the period of the Arnold map;

3. design of a new confusion operation dependent on RSA and acting as one part of the confusion-substitution structure in a cipher;

4. achievement of a high-level gray difference that can be applied to shuffle image pixel.

2 Background

2.1 RSA algorithm

Public-key cryptography uses different encryption and decryption keys. Because the encryption key is public, its distribution and management are simple, and digital signatures can be easily implemented. RSA is an efficient algorithm that could be used for both encryption and digital signatures. It is easy to understand and operate. It is also the most widely researched public-key algorithm, and has withstood various attacks. Algorithm 1 shows the RSA encryption and decryption process.

Algorithm 1 RSA encryption and decryption

Input: prime numbers p and q and plaintext information m

Output: ciphertext information c

1: Calculate $n = pq$ and $\varphi(n) = (p-1)(q-1)$
2: Randomly select public key e satisfying $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$
3: Calculate the private key d, i.e., $d \equiv e^{-1} \bmod \varphi(n)$
4: Encryption: $c = m^e \bmod n$
5: Decryption: $m = c^d \bmod n$

This public-key system has two types of keys: $\{e, n\}$ is the public key and $\{p, q, d\}$ is the private (secret) key. In data transmission, the sender knows the receiver's public key and uses it to encrypt the message. The receiver uses their own private key to decrypt the ciphertext and obtain the plaintext message.

2.2 Arnold transform

The Arnold map was proposed in the ergodic theory of classical mechanics, and is commonly known as the cat-face transformation. As to physical meaning, Arnold transform is a chaotic mapping method that repeatedly conducts folding, splicing, and stretching of transformation in a limited area. Through transformation, points in the discrete

digital image matrix are rearranged into a new confused image matrix. That is to say, it changes the pixel coordinates of the digital image and perturbs the image, making the digital image appear as white noise. Its definition is as follows:

Suppose that the size of the original image is $N \times N$, with (x_n, y_n) as the coordinates of a pixel in the original image and (x_{n+1}, y_{n+1}) the position after transformation. The transformation formula is expressed as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N. \quad (1)$$

The digital image is treated as a matrix and the original image will be scrambled. Then, the inverse transformation can be used to restore the original image. The corresponding inverse transformation formula is as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N. \quad (2)$$

However, the Arnold transform is periodic, and the image will return to its original state after a certain number of transformation iterations; hence, the confusion number is important. The periodicity of the Arnold transform is related to the image size, so it is difficult to recover the original image if one fixes the iteration number to any image size.

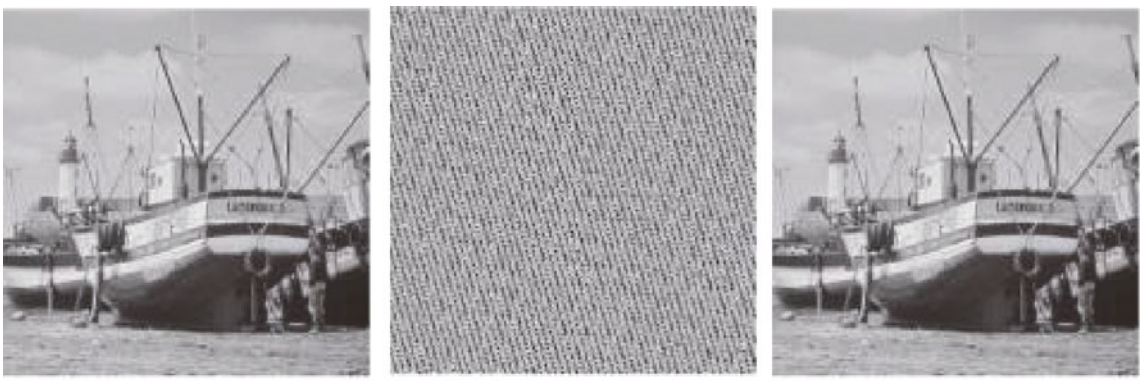
Table 1 shows the relationship between Arnold transform period T and size N (Chen LF et al., 2013). To improve the security of image confusion, the execution period of the Arnold transform and size N are fixed as different values. Fig. 1 shows the results of Arnold transform after different execution periods (supposing $a = 5$ and $b = 3$). In Fig. 1a, the Boat image is 256×256 pixels, so according to Table 1, its period is 192. Fig. 1b shows the results after 50 rounds of Arnold transform, and Fig. 1c shows the recovered image after 192 rounds of Arnold transform. Simulation results validate well the periodic relationships shown in Table 1.

2.3 Fast calculation method

In the RSA algorithm, encryption and decryption both need to conduct large-integer modular power multiplication. To simplify the calculations and increase the operation speed, a fast calculation method (FCM) (Hui and Lam, 1994) is adopted in our study. In the $\theta = a^e \bmod n$ calculation, e is expressed in a binary form; i.e., $e = \sum_{i=0}^{k-1} e_i 2^i$, where $e_i \in \{0, 1\}$ and k is the number of bits used by e in the binary. Then, an iterative operation is carried out. The specific calculation process is shown in Algorithm 2. Table 2 shows the time comparison between the traditional method

Table 1 Relationship between the Arnold transform period T and size N

N	T	N	T	N	T
2	3	32	24	33	20
3	4	64	48	65	70
4	3	128	96	100	150
5	10	256	192	257	258
6	12	512	384	513	1432
7	8	1024	768	1025	100
8	6	2048	1536	2049	684
9	12	4096	3072	4097	360
10	30	8192	6144	8193	780



(a) (b) (c)

Fig. 1 Image confusion test for Boat: (a) original image; (b) results after 50 rounds of Arnold transform; (c) result after 192 rounds of Arnold transform

Algorithm 2 Fast calculation method

Input: a, e, and n
Output: θ

```
Transfer e = dec2bin(e)
Obtain k = length(e)
Set m = 1
for i = 1 : k do
    m = m^2 mod n
    if e(i) == 1 then
        m = (m × a) mod n
    end if
end for
Obtain θ = m
```

Table 2 Time comparison between the traditional method (TM) and the fast calculation method (FCM)

Method	Time (s)			
	Case 1	Case 2	Case 3	Case 4
TM	0.0683	0.0546	0.0663	0.0772
FCM	0.0315	0.0399	0.0485	0.0471

and the FCM when calculating the modular multiplication in four cases: case 1, $254\ 208^{341\ 923}$ mod 818 627; case 2, $539\ 916^{220\ 265}$ mod 818 627; case 3, $203\ 350^{419\ 411}$ mod 751 589; Case 4, $168\ 807^{491\ 285}$mod 751 589.

3 The proposed asymmetric confusion algorithm

3.1 Image confusion process

This scheme is based on the RSA asymmetric public-key system and the Arnold confusion operation, and an effective image-confusion method is proposed. This study is concerned mainly with image confusion technology. Scrambling in cryptography initially hides the image information by changing the positions of pixels in the image. The confusion algorithm is shown in Algorithm 3. The image confusion process is shown in Fig. 2.

The confusion process proceeds as follows:

Step 1: use the RSA algorithm to generate private key d and public key e.

Step 2: read the original image as P. Randomly select two positive integers a_1 and a_2, and encrypt them with the generated public key. Calculate the open ciphertext information $m_i = a_i^e \bmod n$ $(i = 1, 2)$. Let $s = \sqrt{\log(\sum P_{i,j}^2 + 1)}$, and calculate b through the obtained ciphertext. That is, given a_1 and a_2, the formula for generating parameter values

Algorithm 3 The proposed image confusion algorithm

Input: P (original image), a_1, and a_2
Output: EI (block confusion image) and C (confused image)

```
Read image P
Obtain the size [M, N] = size(P)
Obtain b1, b2 from a1, a2, respectively
Set blc = zeros(M/2, N/2)
for i = 1 : 2 do
    for j = 1 : 2 do
        x = (i − 1)(M/2) + 1,  y = (j − 1)(N/2) + 1
        blc = P(x : x + M/2 − 1, y : y + N/2 − 1)
        Do Arnold transform using the first group a1
        and b1 for blc
        EI(x : x + M/2 − 1, y : y + N/2 − 1) = blc
    end for
end for
Confuse EI using the second group a2 and b2 by
Arnold transform to obtain C
Return confused image C
```

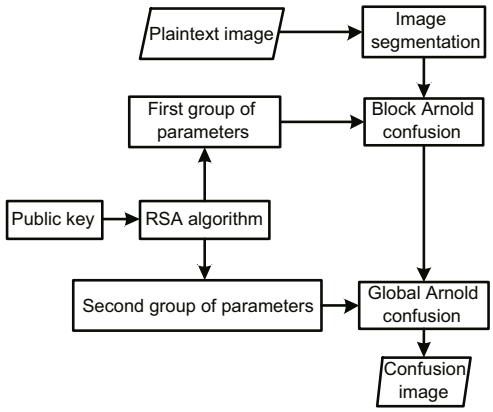


Fig. 2 Asymmetric image confusion algorithm

b_1 and b_2 is as follows:

$$\begin{cases} m_i = a_i^e \bmod n, \\ s = \sqrt{\log(\sum P_{i,j}^2 + 1)}, \\ b_i = \mathrm{fix}(a_i + \sqrt{\log m_i + s}), \end{cases} \tag{3}$$

where $\mathrm{fix}(x)$ returns the integer of x.

Step 3: divide the image into four blocks. Substitute the first parameter group a_1 and b_1 into the Arnold transform formula and take Arnold confusion for each sub-block to obtain the block confusion image B.

Step 4: substitute the second parameter group a_2 and b_2 into the Arnold transform formula and repeat the Arnold transform on the entire image to obtain the final confused image C.

3.2 Reverse image confusion process

The reverse image confusion process involves the following steps:

Step 1: decrypt the public ciphertext information m_i $(i = 1, 2)$ with private key d, i.e., $a_i = m_i^d \bmod n$ $(i = 1, 2)$. Use Eq. (3) to obtain two groups of parameters for the reverse process.

Step 2: substitute the second group a_2 and b_2 into Eq. (2) and perform the Arnold inverse transform on the confused image C to obtain B'.

Step 3: divide image B' into four blocks. Then, substitute the first group a_1 and b_1 into Eq. (2) to obtain the original image P' by executing the Arnold confusion operation on each sub-block.

4 Experimental results

In this study, four standard greyscale images were selected for testing. The work was simulated using MATLAB R2017b on the Windows 10 operating system. The following large prime numbers were selected: $p = 859$, $q = 953$. Then, $a_1 = 5$, $a_2 = 9$, $b_1 = 13$, and $b_2 = 17$ were obtained by testing the Peppers image. The block confusion number was set to 20, and the global confusion number was set to 30. The Peppers image in Fig. 3a was in the size of 512×512 pixels. Fig. 3b is the block confusion image of Fig. 3a, and Fig. 3c is the final confusion image of Fig. 3a. Fig. 3d shows the overall inverse confusion image when the wrong key $a_1 = 4$ was used. Fig. 3e is the block inverse confusion image when the wrong key $a_1 = 4$ was used. Fig. 3f is the image when the correct key was used. The image test results show that if the wrong key is used, the original image information cannot be obtained.

5 Confusion analysis

5.1 Correlation analysis

One of the most important differences between images and text is the correlation (Zhou et al., 2014; Zhu HH et al., 2019) of two adjacent digital messages. In meaningful images, there is a high correlation between pixels and their neighbors in the horizontal, vertical, and diagonal directions. The aim of the scrambling technique is to break the correlation between adjacent pixels in all three directions, to achieve an image with the maximum randomness and zero or the minimum correlation. To measure the correlation coefficient between two adjacent pixels, the following formulae are used:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)], \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)], \tag{6}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}[y_i - E(y)], \tag{7}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{8}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i, \tag{9}$$

where x_i and y_i represent the gray values of two images, r_{xy} represents the correlation coefficient, x and y are the gray values of two adjacent pixels, and N is the total logarithm of (x_i, y_i). The correlation coefficient between the original image and the corresponding encrypted image is shown in Fig. 4. Table 3 shows the correlation coefficients for the vertical, horizontal, and diagonal directions for all the test images.

In addition, we compare the proposed algorithm with the traditional Arnold method (TAM). Table 4 shows the comparison results. The test results show that the correlation coefficient of the confused image is close to zero. Therefore, there is no relationship between adjacent image pixels.

Table 3 Correlation coefficients of different images

Image		Correlation coefficient		
		Horizontal	Vertical	Diagonal
Plaintext image	Boat	0.9372	0.9240	0.8790
	Man	0.9638	0.9336	0.9137
	Baboon	0.9135	0.9323	0.8746
	Peppers	0.9517	0.9447	0.9168
Confusion image	Boat	0.0141	−0.1020	0.0363
	Man	0.0629	0.0191	0.0347
	Baboon	−0.0483	−0.0338	−0.0613
	Peppers	−0.0131	−0.0147	−0.0039

Table 4 Correlation coefficients of different algorithms for the Boat image

Direction	Correlation coefficient		
	Original image	Ours	TAM
Horizontal	0.9372	0.0141	−0.2401
Vertical	0.9240	−0.1020	0.4071
Diagonal	0.8790	0.0363	−0.2491

TAM: traditional Arnold method

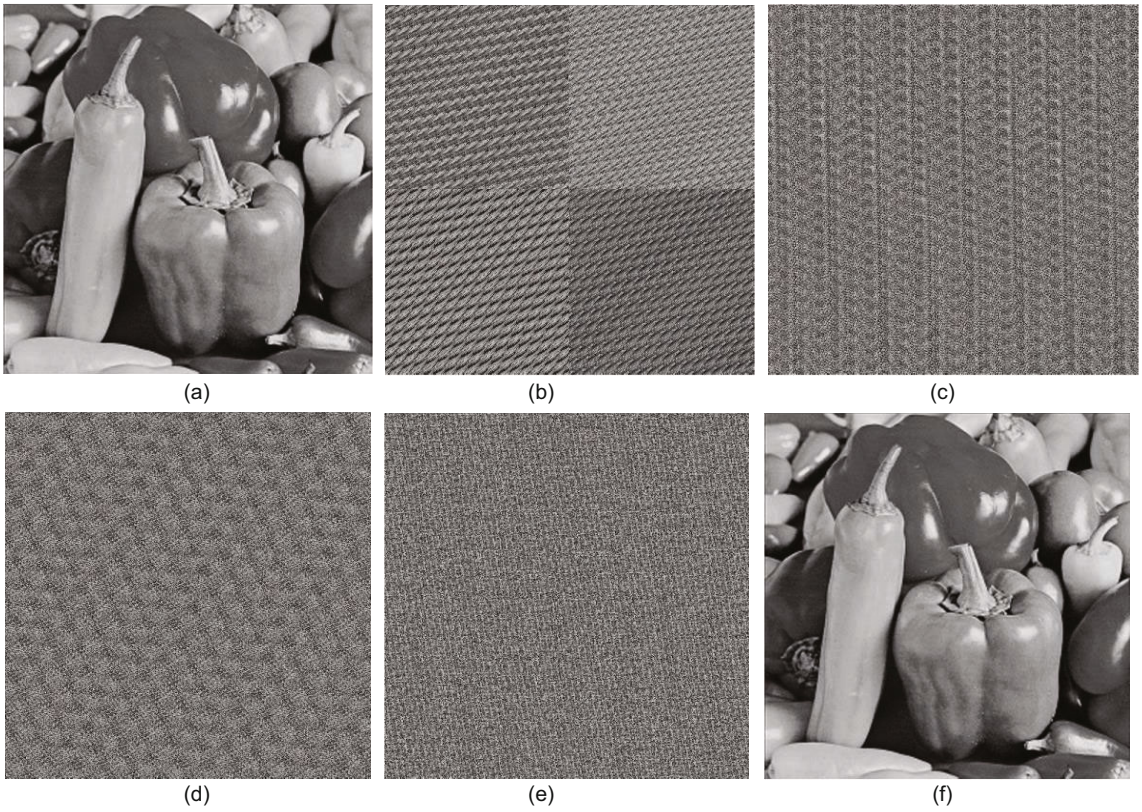


Fig. 3 Image confusion and inverse confusion tests using the new algorithm: (a) original image; (b) block confusion image; (c) confused image; (d) overall inverse confusion image with the wrong key; (e) block inverse confusion image with the wrong key; (f) inverse confusion image with the correct key

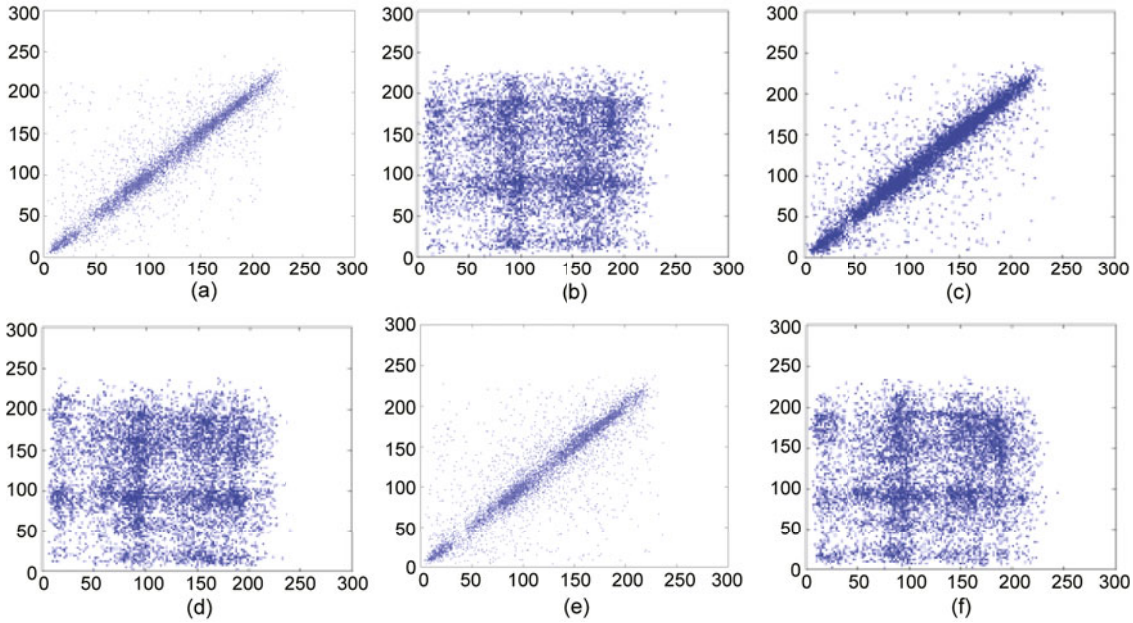


Fig. 4 Correlation of adjacent pixels in the Peppers image: (a) original image in the horizontal direction; (b) confused image in the horizontal direction; (c) original image in the vertical direction; (d) confused image in the vertical direction; (e) original image in the diagonal direction; (f) confused image in the diagonal direction

5.2 Key sensitivity analysis

The security key analysis reveals the sensitivity to the security key (Méndez-Ramírez et al., 2018). The sensitivity is considered from two aspects: whether a small change in the security key will make a significant difference in the confused image and whether the image can be recovered with other keys. Four standard images are confused with the same key, and the global confusion number in the key is set to 30.

Figs. 5a–5d show 30 times global confusion images for Boat, Man, Baboon, and Peppers. If the number of global confusion times is 31 for inverse confusion, Figs. 5e–5h show the corresponding inverse confusion images, indicating that the clear text information cannot be recovered. Simultaneously, to further test its sensitivity, the standard image is confused with keys $a_1 = 5$ and $a_2 = 9$, and the resulting image is anti-confused with keys $a_1 = 4$ and $a_2 = 10$. Fig. 6 shows the confusion and inverse confusion results of the four standard images.

5.3 Security analysis

The security of this method is based on the security of the RSA asymmetric system, which depends on the factorization of large integers. Trying to decompose the prime factor of modulus n is the most direct way to attack RSA. To improve the security, the parameter choice is important. p and q should be strong prime numbers. The difference between these two numbers should be as large as possible, and the value should be large enough to make factorization impossible.

Factorization is one of the most common problems in cryptography. Although factorization algorithms have made great progress, there is still not enough evidence to prove that RSA can be cracked. Therefore, as long as n reaches a certain requirement and parameters p, q, and e are reasonably selected, a system based on RSA is safe.

5.4 Period analysis

The periodicity of an Arnold map is related to the size of the image. In this study, we adopt the block-by-block and the whole methods. After the image is divided into blocks (block-by-block), the confusion period of each sub-block is changed. We take image size 128×128 as an example. When N is 128, the period is 96. If the image is divided into four blocks, each block's size is 64×64. Therefore, the period of each block is 48, and the entire period is $64 \times 48 = 3072$. Table 5 shows the transformation period comparison between our method and the traditional method.

Table 5 Transformation period comparison between our method and the traditional method

N	T	
	Our method	Ttraditional method
4	9	3
6	4	12
8	18	6
10	300	30
12	144	12
16	72	12
32	288	24
50	6000	150
64	1152	48
128	4608	96
256	18 432	192
512	73 728	384

5.5 Gray difference and its comparisons

The adjacent gray difference (Ye, 2010) is used to scramble each pixel of the image, so that the difference between the pixel values of any pixel and its neighboring pixels tends to be as large as possible. The larger the value, the better the effect of adjacent gray difference scrambling. The formula for calculating the difference in gray values between image pixels and neighboring pixels is expressed as

$$\mathrm{GD} = \frac{\sum[G(x,y) - G'(x',y')]^2}{4}, \tag{10}$$

where $(x', y') = \begin{cases} (x-1, y) \\ (x+1, y) \\ (x, y-1) \\ (x, y+1) \end{cases}$ and $G(x, y)$ represents the gray value at position (x, y). Excluding the pixels on the edge of the image, the average neighborhood gray difference of the remaining pixels in the image is calculated as

$$E(\mathrm{GD}(x,y)) = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1}\mathrm{GD}(x,y)}{(M-2)(N-2)}. \tag{11}$$

The calculation formula for the gray-value scrambling degree (Ye, 2010) is

$$\mathrm{GVD} = \frac{E'(\mathrm{GD}(x,y)) - E(\mathrm{GD}(x,y))}{E'(\mathrm{GD}(x,y)) + E(\mathrm{GD}(x,y))}, \tag{12}$$

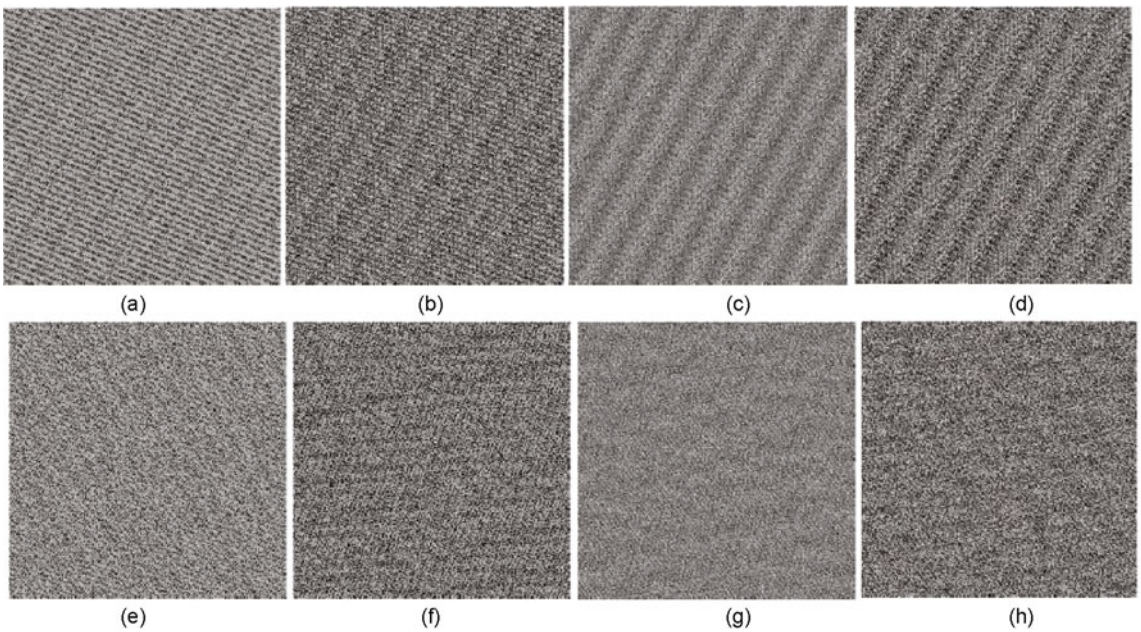


Fig. 5 Confusion images with 30 times global confusion: (a) Boat; (b) Man; (c) Baboon; (d) Peppers. Inverse confusion images with 31 times global confusion: (e) Boat; (f) Man; (g) Baboon; (h) Peppers

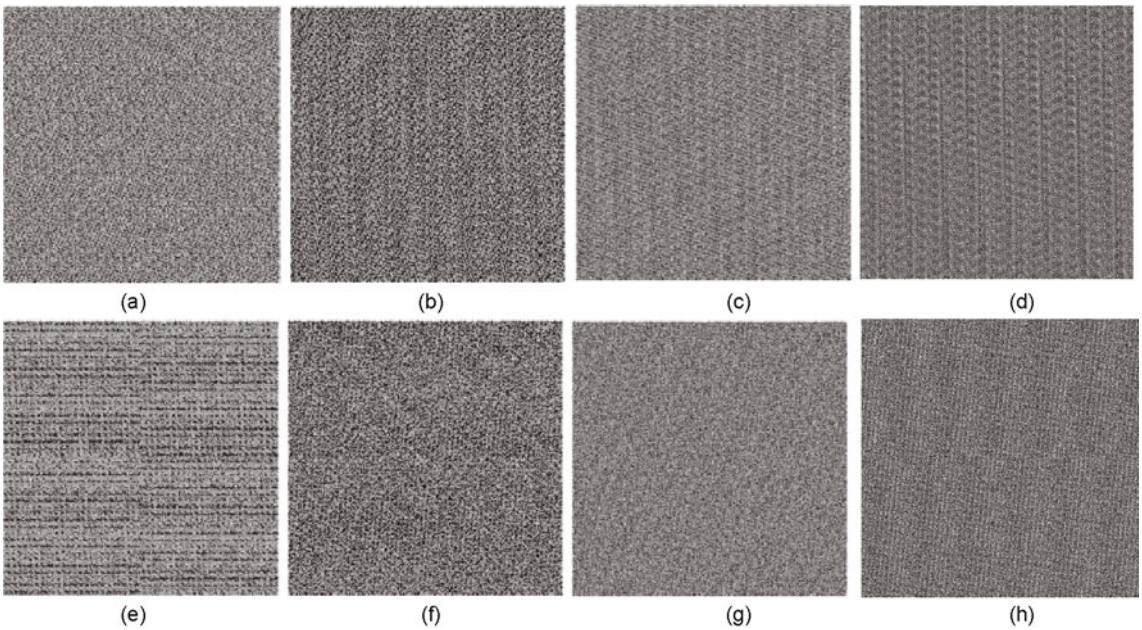


Fig. 6 Confusion with keys $a_1 = 5$ and $a_2 = 9$: (a) Boat; (b) Man; (c) Baboon; (d) Peppers. Inverse confusion with keys $a_1 = 4$ and $a_2 = 10$: (e) Boat; (f) Man; (g) Baboon; (h) Peppers

where E and E' are the average neighborhood gray differences of the image before and after scrambling, respectively.

Three different methods, i.e., our method, Arnold method (Abbas, 2016), row-column exchange method (R-C) (Patidar et al., 2011), are used to compare the odd values of the same image in 25 iterations. Table 6 shows the comparison of the gray values of these three sample images. It can be seen that the proposed method performs the best.

Taking the 256×256 Boat image as an example, the gray differences of different methods are analyzed and compared. Fig. 7 shows the comparison of the scrambling degree using double cycles of

the traditional Arnold map based method and our method. It is easy to see that most values are less than 0.875 using the traditional Arnold map, while our method displays better performance with values larger than 0.90. Fig. 8 shows the comparison of the confusion degree among the proposed algorithm, the R-C method, and the traditional Arnold method with one circle. The proposed method has higher confusion degree.

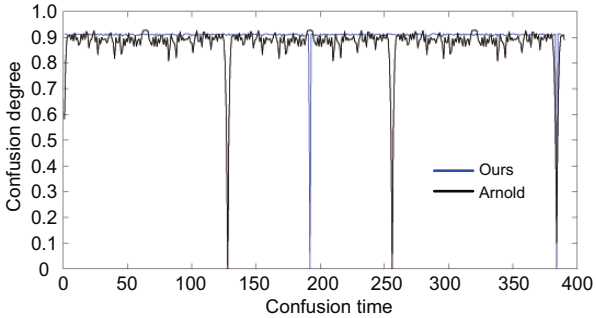


Fig. 7 Comparison of the gray value confusion degree with double cycles

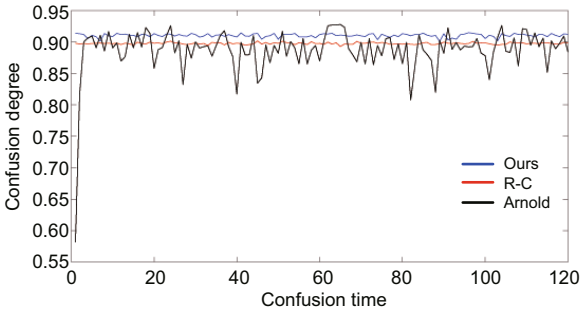


Fig. 8 Comparison of the gray value confusion degree with three methods in one cycle

6 Conclusions

The public-key algorithm separates the encryption and decryption keys, reduces the number of keys required for multi-user communication, saves system resources, and facilitates key management. Image confusion is a means to hide information. Considering the security of the confusion algorithm, a new asymmetric image pixel confusion algorithm was proposed based on RSA and the Arnold map. Public and private keys were generated using the RSA algorithm, and then the image's pixels were confused. The Arnold confusion method was used on the image blocks first, and then the entire image was confused to enhance the confusion effect. The experimental results showed that the proposed algorithm is simple to implement and has high confusion degree with test values near to one.

Contributors

Xiao-ling HUANG and Guo-dong YE designed the research and provide suggestions. Kai-xin JIAO processed the data and drafted the manuscript. You-xia DONG helped organize the manuscript. Kai-xin JIAO and Guo-dong YE revised and finalized the paper.

Compliance with ethics guidelines

Xiao-ling HUANG, You-xia DONG, Kai-xin JIAO, and Guo-dong YE declare that they have no conflict of interest.

References

Abbas NA, 2016. Image encryption based on independent component analysis and Arnold's cat map. *Egypt*

Table 6 Comparison of the gray differences for different images

Round number	Gray value								
	Boat			Baboon			Peppers		
	Ours	Arnold	R-C	Ours	Arnold	R-C	Ours	Arnold	R-C
1	0.9138	0.5814	0.8982	0.8742	0.5648	0.8479	0.9091	0.5807	0.8977
3	0.9120	0.9003	0.8969	0.8757	0.8229	0.8488	0.9048	0.8229	0.8986
5	0.9106	0.9095	0.8967	0.8698	0.8990	0.8590	0.9045	0.8990	0.8967
7	0.9017	0.9106	0.8997	0.8958	0.8929	0.8535	0.8994	0.8929	0.8980
9	0.9099	0.9166	0.8973	0.8894	0.8905	0.8561	0.9047	0.8905	0.8974
11	0.9138	0.8985	0.9013	0.8865	0.8907	0.8587	0.9056	0.8907	0.9001
13	0.9126	0.8766	0.8996	0.8922	0.8453	0.8605	0.9048	0.9053	0.8949
15	0.9105	0.8908	0.9010	0.8798	0.8398	0.8513	0.9023	0.8798	0.8977
17	0.9122	0.8921	0.8958	0.8663	0.8379	0.8574	0.9071	0.8779	0.8983
19	0.9083	0.9138	0.9012	0.8827	0.8981	0.8484	0.9019	0.8981	0.8982
21	0.9013	0.8879	0.8997	0.8941	0.8930	0.8528	0.9072	0.9030	0.8970
23	0.9104	0.9098	0.8983	0.8720	0.8565	0.8574	0.9064	0.8865	0.8968
25	0.9094	0.8827	0.8973	0.8933	0.8905	0.8434	0.9045	0.8905	0.8973

Inform J, 17(1):139-146.
https://doi.org/10.1016/j.eij.2015.10.001

Arab A, Rostami MJ, Ghavami B, 2019. An image encryption method based on chaos system and AES algorithm. *J Supercomput*, 75(10):6663-6682.
https://doi.org/10.1007/s11227-019-02878-7

Boldyreva A, Imai H, Kobara K, 2010. How to strengthen the security of RSA-OAEP. *IEEE Trans Inform Theory*, 56(11):5876-5886.
https://doi.org/10.1109/TIT.2010.2070330

Chen JX, Zhu ZL, Zhang LB, et al., 2018. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. *Signal Process*, 142:340-353.
https://doi.org/10.1016/j.sigpro.2017.07.034

Chen LF, Zhao DM, Ge F, 2013. Image encryption based on singular value decomposition and Arnold transform in fractional domain. *Opt Commun*, 291:98-103.
https://doi.org/10.1016/j.optcom.2012.10.080

El-Khamy SE, Korany NO, El-Sherif MH, 2017. A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. *Multim Tool Appl*, 76(22):24091-24106.
https://doi.org/10.1007/s11042-016-4113-8

Gan ZH, Chai XL, Han DJ, et al., 2019. A chaotic image encryption algorithm based on 3-D bit-plane permutation. *Neur Comput Appl*, 31(11):7111-7130.
https://doi.org/10.1007/s00521-018-3541-y

Gong LH, Qiu KD, Deng CZ, et al., 2019a. An image compression and encryption algorithm based on chaotic system and compressive sensing. *Opt Laser Technol*, 115:257-267.
https://doi.org/10.1016/j.optlastec.2019.01.039

Gong LH, Qiu KD, Deng CZ, et al., 2019b. An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Opt Laser Eng*, 121:169-180.
https://doi.org/10.1016/j.optlaseng.2019.03.006

Hua ZY, Xu BX, Jin F, et al., 2019. Image encryption using Josephus problem and filtering diffusion. *IEEE Access*, 7:8660-8674.
https://doi.org/10.1109/ACCESS.2018.2890116

Hui LCK, Lam KY, 1994. Fast square-and-multiply exponentiation for RSA. *Electron Lett*, 30(17):1396-1397.

Khashan OA, Zin AM, Sundararajan EA, 2015. ImgFS: a transparent cryptography for stored images using a filesystem in userspace. *Front Inform Technol Electron Eng*, 16(1):28-42.
https://doi.org/10.1631/FITEE.1400133

Li P, Xu J, Mou J, et al., 2019. Fractional-order 4D hyperchaotic memristive system and application in color image encryption. *EURASIP J Image Video Process*, 2019:22. https://doi.org/10.1186/s13640-018-0402-7

Liu LF, Hao SD, Lin J, et al., 2018. Image block encryption algorithm based on chaotic maps. *IET Signal Process*, 12(1):22-30. https://doi.org/10.1049/iet-spr.2016.0584

Liu ZJ, Gong M, Dou YK, et al., 2012. Double image encryption by using Arnold transform and discrete fractional angular transform. *Opt Laser Eng*, 50(2):248-255.
https://doi.org/10.1016/j.optlaseng.2011.08.006

Mansouri A, Wang XY, 2020. Image encryption using shuffled Arnold map and multiple values manipulations. *Vis Comput*. https://doi.org/10.1007/s00371-020-01791-y

Méndez-Ramírez R, Arellano-Delgado A, Cruz-Hernández C, et al., 2018. Chaotic digital cryptosystem using serial peripheral interface protocol and its dsPIC implementation. *Front Inform Technol Electron Eng*, 19(2):165-179. https://doi.org/10.1631/FITEE.1601346

Mitchell CJ, 2016. On the security of 2-key triple DES. *IEEE Trans Inform Theory*, 62(11):6260-6267.
https://doi.org/10.1109/TIT.2016.2611003

Mossa E, 2017. Security enhancement for AES encrypted speech in communications. *Int J Speech Technol*, 20(1):163-169.
https://doi.org/10.1007/s10772-017-9395-3

Patidar V, Pareek NK, Purohit G, et al., 2011. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Opt Commun*, 284(19):4331-4339.
https://doi.org/10.1016/j.optcom.2011.05.028

Rawat N, Kim B, Kumar R, 2016. Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique. *Optik*, 127(4):2282-2286.
https://doi.org/10.1016/j.ijleo.2015.11.064

Sneha PS, Sankar S, Kumar AS, 2020. A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. *J Amb Intell Human Comput*, 11(3):1289-1308.
https://doi.org/10.1007/s12652-019-01385-0

Verma G, Liao MH, Lu DJ, et al., 2019. An optical asymmetric encryption scheme with biometric keys. *Opt Laser Eng*, 116:32-40.
https://doi.org/10.1016/j.optlaseng.2018.12.010

Wu C, Hu LY, Wang Y, et al., 2019. Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain. *Opt Commun*, 448:26-32.
https://doi.org/10.1016/j.optcom.2019.05.009

Xiao D, Wang Y, Xiang T, et al., 2017. High-payload completely reversible data hiding in encrypted images by an interpolation technique. *Front Inform Technol Electron Eng*, 18(11):1732-1743.
https://doi.org/10.1631/FITEE.1601067

Yao LL, Yuan CJ, Qiang JJ, et al., 2017. An asymmetric color image encryption method by using deduced gyrator transform. *Opt Laser Eng*, 89:72-79.
https://doi.org/10.1016/j.optlaseng.2016.06.006

Ye GD, 2010. Image scrambling encryption algorithm of pixel bit based on chaos map. *Patt Recogn Lett*, 31(5):347-354.
https://doi.org/10.1016/j.patrec.2009.11.008

Ye GD, Huang XL, 2018. Spatial image encryption algorithm based on chaotic map and pixel frequency. *Sci China Inform Sci*, 61(5):058104.
https://doi.org/10.1007/s11432-017-9191-x

Ye GD, Pan C, Huang XL, et al., 2018. An efficient pixel-level chaotic image encryption algorithm. *Nonl Dynam*, 94(1):745-756.
https://doi.org/10.1007/s11071-018-4391-y

Yu SS, Zhou NR, Gong LH, et al., 2020. Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system.

Opt Laser Eng, 124:105816.
https://doi.org/10.1016/j.optlaseng.2019.105816

Zhou NR, Zhang AD, Zheng F, et al., 2014. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Opt Laser Technol*, 62:152-160.
https://doi.org/10.1016/j.optlastec.2014.02.015

Zhou NR, Hua TX, Gong LH, et al., 2015. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. *Quant Inform Process*, 14(4):1193-1213.
https://doi.org/10.1007/s11128-015-0926-z

Zhu HH, Chen XB, Yang YX, 2019. A quantum image dual-scrambling encryption scheme based on random permutation. *Sci China Inform Sci*, 62(12):229501.
https://doi.org/10.1007/s11432-018-1514-y

Zhu ZL, Zhang W, Wong KW, et al., 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inform Sci*, 181(6):1171-1186.
https://doi.org/10.1016/j.ins.2010.11.009